

Relativized Worlds with an Infinite Hierarchy*

Lance Fortnow[†]
University of Chicago
Department of Computer Science
1100 E. 58th. St.
Chicago, IL 60637

Abstract

We introduce the “Book Trick” as a method for using results about random oracles to create relativized worlds with an infinite polynomial-time hierarchy. We use it to show, for example, a single relativized world where

- One can find satisfying assignments to satisfiable formulae with only nonadaptive queries to an **NP** oracle, and
- the counting class **SPP** strictly contains the polynomial-time hierarchy, and
- the polynomial-time hierarchy is infinite.

Keywords: Theory of Computation; Computational Complexity; Relativization; Polynomial-Time Hierarchy; Ronald Book

1 Introduction

Creating a relativized world where the polynomial-time hierarchy is infinite was one of the more difficult constructions in the mid-1980’s. The field of circuit complexity was invented initially to tackle this problem (see [FSS84]). The first such construction by Yao [Yao85] was a technical masterpiece.

These days we often have the task of making some other proposition true while making the polynomial-time hierarchy infinite. Consider, for example, the following proposition.

Proposition 1.1 *One can find satisfying assignments to satisfiable formulae using nonadaptive queries to an **NP** oracle.*

Finding satisfying assignments using an **NP** oracle is an easy process using the self-reducing properties of **SAT**. However this algorithm requires adaptive queries to **SAT**.

One might conjecture that Proposition 1.1 implies the polynomial-time hierarchy collapses. We would like to give a relativized counterexample to this conjecture, i.e., create a relativized world where Proposition 1.1 holds and the polynomial-time hierarchy is infinite.

*This paper is dedicated to the memory of Ronald Book. May his love of structural complexity theory and his desire to share it with the world be an inspiration to us all.

[†]URL: <http://www.cs.uchicago.edu/~fortnow>. Email: fortnow@cs.uchicago.edu. Supported in part by NSF grant CCR 92-53582.

Creating such worlds is still a difficult task. One can try a direct construction, using such combinatorial techniques such as the Håstad switching lemma [Hås89] but these approaches are complicated at best. Another useful but limited direction involves generic oracles (see [FFKL93]).

In this paper, we introduce a new technique using random oracles. We show how to use a recent result by Ron Book to turn results on random oracles to results on oracles that make the polynomial-time hierarchy infinite.

Ron Book [Boo94] showed that if the polynomial-hierarchy collapses relative to a random oracle then it collapses unrelativized. We use this result to formulate a technique we call the *Book Trick*:

Any relativizing proof that a proposition holds relative to a random oracle immediately implies that there exists an oracle that makes the proposition true and simultaneously makes the polynomial-time hierarchy infinite.

Watanabe and Toda [WT93] give a relativizable proof that Proposition 1.1 holds relative to a random oracle. Using our techniques, we immediately get that there exists a relativized world where the polynomial-time hierarchy is infinite and Proposition 1.1 holds.

We also examine the counting class **SPP** defined by Fenner, Fortnow and Kurtz [FFK94] and give a relativized world where **SPP** strictly contains an infinite polynomial-time hierarchy.

2 Preliminaries

We assume the reader is familiar with Turing machines and standard complexity classes such as **P**, **NP** and **coNP** and the concept of relativization. Fortnow [For94] gives an overview of relativization and its importance in complexity theory.

The polynomial-time hierarchy is a generalization of **NP** defined inductively. We let $\Sigma_0^p = \mathbf{P}$ and $\Sigma_{i+1}^p = \mathbf{NP}^{\Sigma_i^p}$ for $i \geq 0$. We let $\mathbf{PH} = \bigcup_{i \geq 0} \Sigma_i^p$. We say the polynomial-time hierarchy *collapses* if $\Sigma_i^p = \Sigma_{i+1}^p$ for some i , otherwise we say the polynomial-time hierarchy is *infinite*. Most complexity theorists conjecture that the polynomial-time hierarchy is infinite.

We let $\chi_L(x)$ be the *characteristic function* of L , i.e., $\chi_L(x) = 1$ if x is in L and $\chi_L(x) = 0$ otherwise.

Let $\langle x, y \rangle$ be a standard polynomial-time computable and invertible tupling function.

We use $A \oplus B$ to represent the *join* of A and B , i.e.,

$$A \oplus B = \{\langle x, i \rangle \mid (i = 0 \text{ and } x \in A) \text{ or } (i = 1 \text{ and } x \in B)\}.$$

We use $A \Delta B$ to be the disjoint union of A and B , i.e. $A \Delta B = (A - B) \cup (B - A)$.

3 The Book Trick

Creating relativized worlds where the polynomial-time hierarchy is infinite is a difficult process requiring combinatorial bounds on bounded depth circuits. The first such oracle is due to Yao [Yao85].

Theorem 3.1 (Yao) *There exists an oracle A such that for all $i \geq 0$, $\Sigma_i^A \neq \Sigma_{i+1}^A$.*

His proof has been simplified and improved by Håstad [Hås89].

Because of the difficulty of the construction, complexity theorists have had little luck creating relativized worlds where the polynomial-time hierarchy is infinite and other specific complexity statements hold. One notable exception is the work of Sheu and Long [SL96] separating the low and high hierarchies.

We show how to use the theory of random oracles to help create relativized worlds where the polynomial-time hierarchy is infinite. Bennet and Gill [BG81] first looked at random oracles.

Definition 3.2 (Bennet-Gill) *A relativizable proposition \mathcal{P} holds relative to a random oracle if*

$$\Pr_{R \subseteq \{0,1\}^*}(\mathcal{P}^R) = 1.$$

Bennet and Gill show that $\mathbf{P} \neq \mathbf{NP}$ relative to a random oracle.

Many complexity theorists had believed in the “random oracle hypothesis” where propositions holding relative to a random oracle should also hold in the unrelativized world. Recent work on interactive proofs have put that hypothesis to rest (see [CCG⁺94]).

Still we can use tools for random oracles to show that certain relativized worlds exist. One of these tools is the Kolmogorov Zero-One law.

Lemma 3.3 *If \mathcal{P} is a relativizable proposition such that $\mathcal{P}^A \Leftrightarrow \mathcal{P}^{A\Delta B}$ for all oracles A and finite sets B then*

$$\Pr_{R \subseteq \{0,1\}^*}(\mathcal{P}^R) \in \{0, 1\}.$$

Since we can encode finite differences of an oracle in the code of a Turing machine, nearly all propositions \mathcal{P} have the property needed for Lemma 3.3.

Ron Book [Boo94] proves the following result.

Theorem 3.4 (Book) *If relative to random R the polynomial-time hierarchy collapses then the (unrelativized) polynomial-time hierarchy collapses.*

A close examination of Book’s proof and the proof of Nisan and Wigderson [NW94] that Book uses shows that Theorem 3.4 relativizes. Also for our purposes, the contrapositive will be a more useful form for us. This yields the following corollary.

Corollary 3.5 (Book) *For every oracle A , if the polynomial-time hierarchy is infinite relative to A then for random R , the polynomial-time hierarchy relative to $A \oplus R$ is infinite.*

From Corollary 3.5 we can then turn relativizable theorems about random oracles into results about an infinite polynomial-time hierarchy.

Lemma 3.6 (The Book Trick) *If \mathcal{P} is a relativizable proposition such that for all A and random R , $\mathcal{P}^{A\oplus R}$ is true then there exists an oracle B such that \mathcal{P}^B holds and the polynomial-time hierarchy is infinite relative to B .*

Proof: By Theorem 3.1, let A be an oracle relative to which the polynomial-time hierarchy is infinite. Then for random R we have $\mathcal{P}^{A\oplus R}$ and the polynomial-time hierarchy is infinite relative to $A \oplus R$. Fix such an R and let $B = A \oplus R$. \square

Note that Lemma 3.6 does *not* imply that the polynomial-time hierarchy is infinite relative to a random oracle. This remains an important unproven conjecture.

We can immediately apply Lemma 3.6 to give us many interesting relativized worlds.

Corollary 3.7 *There exists a single relativized world where*

- **NP** does not have measure zero in **EXP**,
- One can find a satisfying assignment of a satisfiable formula with nonadaptive queries to **NP**,
- **P** = **BPP**,
- and the polynomial-time hierarchy is infinite.

The definitions and motivation of measure within **EXP** is beyond the scope of this paper. We recommend the survey by Lutz [Lut97].

Buhrman and Thierauf [BT96] give the first report of an oracle relative to which one can find a satisfying assignment of a satisfiable formula with nonadaptive queries to **NP** and the polynomial-time hierarchy is infinite. We give the first proof in this paper.

Proof of Corollary 3.7: Kautz and Miltersen [KM96], Watanabe and Toda [WT93] and Bennet and Gill [BG81] respectively show that the first three statements hold relative to a random oracle and all of their proofs relativize. Corollary 3.7 immediately follows from Lemma 3.6. \square

We can extend Corollary 3.7 to most statements known to hold relativize to a random oracle such as **NP** = **AM** [NW94], the failure of the Berman-Hartmanis isomorphism conjecture [KMR95], the existence of extremely hard one-way functions [IR89, KMR95] and the existence of disjoint pairs of **NP** (or **coNP**) sets that are not **P**-separable [Ver93].

4 The Complexity of **SPP**

We can also use the Book Trick to show the potential surprising power of the counting class **SPP**.

A function f is a **GapP** function if there exists a polynomial-time nondeterministic Turing machine M such that for all x , $f(x)$ is the difference of the number of accepting computation paths of $M(x)$ and the number of rejecting computation paths of $M(x)$.

Fenner, Fortnow and Kurtz [FFK94] define the **GapP** functions and show many interesting properties of them. They also define the counting class **SPP**.

A language L is in **SPP** if the characteristic function of L is a **GapP** function. Fenner, Fortnow and Kurtz [FFK94] show that in a formal sense **SPP** is the smallest possible nontrivial Gap-definable counting class.

Han, Hemaspaandra and Thierauf [HHT97] examine a class **BPP**_{path} showing

- **BPP**_{path} is contained in the polynomial-time hierarchy, and
- There is a relativized world where **SPP** is not contained in **BPP**_{path}.

A natural question arises as to whether one can simply create a relativized world where **SPP** does not lie in the polynomial-time hierarchy.

Fortnow [For97], in his survey on counting complexity, states the following result without proof.

Theorem 4.1 *There exists a relativized world where **SPP** strictly contains an infinite polynomial-time hierarchy.*

Theorem 4.1 gives an interesting contrast with the following result proven by Fenner, Fortnow, Kurtz and Li [FFKL93] using generic oracles.

Theorem 4.2 *There exists a relativized world where $\mathbf{P} = \mathbf{SPP}$ and the polynomial-time hierarchy is infinite.*

We present the first published proof of Theorem 4.1.

Proof of Theorem 4.1: Toda and Ogihara [TO92] prove the following interesting relationship between the polynomial-time hierarchy and **GapP** functions.

Theorem 4.3 (Toda-Ogihara) *Let f be in $\mathbf{GapP}^{\mathbf{PH}}$ and p be a polynomial. There exist a two-argument function g in \mathbf{GapP} and a polynomial q such that for all x ,*

$$\Pr_{r \in \Sigma^q(n)} (g(x, r) = f(x)) \geq 1 - 2^{-p(n)}.$$

From Theorem 4.3 we can easily show that **SPP** contains **PH** relative to a random oracle. Fix a language L in **PH**. Let f be the characteristic function for L and notice that $f \in \mathbf{GapP}^{\mathbf{PH}}$. Fix $p(n) = 2n + 2$ and let g and q be the results of applying Theorem 4.3.

Let M be the polynomial-time nondeterministic Turing machine that defines the function g . Create a new relativized machine N^R that works as follows: $N^R(x)$ gets r from the oracle by letting $r_i = \chi_R(\langle x, i \rangle)$. The machine will then simulate $M(x, r)$.

Let $h^R(x)$ be the **GapP** function defined by N^R . For any x , the probability over all R that $N^R(x) \neq \chi_L(x)$ is at most $2^{-2|x|+2}$. Summing this error over all strings gives that L is in \mathbf{SPP}^R via f with probability at least $1/2$. By the Kolmogorov zero-one law (Lemma 3.3), we have that L is in \mathbf{SPP}^R for random R .

The above argument relativizes so the Book Trick (Lemma 3.6) gives us a relativized world where **SPP** contains the polynomial-time hierarchy and the hierarchy is infinite. We would then like to apply the following well-known lemma to show strict containment.

Lemma 4.4 *If there exists a set A in the polynomial-time hierarchy such that for every language L in the polynomial-time hierarchy, L polynomial-time many-one reduces to A then the polynomial-time hierarchy collapses.*

Proof: The set A must lie in some Σ_i^p . Let L be a Σ_{i+1}^p -complete set and we then have $\Sigma_i^p = \Sigma_{i+1}^p$. \square

If \mathbf{SPP}^R had a complete set A then by Lemma 4.4, A would not be in the polynomial-time hierarchy and we would have strict containment.

However, we cannot assume \mathbf{SPP}^R has a complete set, in fact there are relativized worlds where **SPP** does not have complete sets (see [FFKL93]).

We get around this problem by analyzing Toda and Ogihara's construction [TO92] for Theorem 4.3. If L_i^R is the standard relativizable complete set for Σ_i^p then the construction produces the machine N above using running time $O(n^{10^i})$. We can then define the relativized set A^R by

$$A^R = \{\langle i, 1^{|x|^{10^i}}, x \rangle \mid x \in L_i^R\}.$$

A simple variation of the above argument shows that $A^R \in \mathbf{SPP}^R$ for random R . Also, we have every language in \mathbf{PH}^R reduces to A so by Lemma 4.4 we have that $A^R \in \mathbf{SPP}^R - \mathbf{PH}^R$ for random R . \square

5 Further Directions

While questions about whether statements hold relative to a random oracle are no longer inherently interesting, they do give us a “probabilistic method” approach to showing the existence of an oracle making a proposition true. Also, by countable additivity of measure zero sets, all statements that hold relative to a random oracle, hold simultaneously relative to a random oracle.

Our paper gives another purpose to studying random oracles: It gives us a method to show that the polynomial-time hierarchy is infinite with respect to many other propositions.

To this end, it is still worthwhile to study the truth of certain statements relative to random oracles, such as

1. Is the polynomial-time hierarchy infinite?
2. Is $\mathbf{P} \neq \mathbf{NP} \cap \mathbf{coNP}$?
3. Is $\mathbf{P} \neq \mathbf{BQP}$ where \mathbf{BQP} is the class of languages accepted efficiently by quantum Turing machines?

Showing the negation of the above would yield surprising results, the first would collapse the hierarchy (Theorem 3.4) and either of the other two would yield a fast probabilistic algorithm for factoring.

Finally, one should realize the limited interpretations of oracle results, particularly for results on interactive proof systems. One can use the Book Trick combined with work of Chang, Chor, Goldreich, Hartmanis, Håstad, Ranjan and Rohatgi [CCG⁺94] to get a relativized world where the polynomial-time hierarchy is infinite and some \mathbf{coNP} languages do not have interactive proofs. However, we know that this result does not hold in the unrelativized world [LFKN92].

Acknowledgments

We thank Harry Buhrman, Lane Hemaspaandra, Thomas Thierauf and Alan Selman for discussions on the Book Trick. We also thank Hemaspaandra for encouraging the author to write this article. Finally we thank the anonymous referees for several suggested improvements on the exposition including the statement of the Book Trick in the introduction.

References

- [BG81] C. Bennett and J. Gill. Relative to a random oracle, $P^A \neq NP^A \neq co - NP^A$ with probability one. *SIAM Journal on Computing*, 10:96–113, 1981.
- [Boo94] R. Book. On collapsing the polynomial-time hierarchy. *Information Processing Letters*, 52(5):235–237, 1994.
- [BT96] H. Buhrman and T. Thierauf. The complexity of generating and checking proofs of membership. In *Proceedings of the 13th Symposium on Theoretical Aspects of Computer Science*, volume 1046 of *Lecture Notes in Computer Science*, pages 75–86. Springer, Berlin, 1996.

- [CCG⁺94] R. Chang, B. Chor, O. Goldreich, J. Hartmanis, J. Håstad, D. Ranjan, and P. Rohatgi. The random oracle hypothesis is false. *Journal of Computer and System Sciences*, 49(1):24–39, August 1994.
- [FFK94] S. Fenner, L. Fortnow, and S. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, 48(1):116–148, 1994.
- [FFKL93] S. Fenner, L. Fortnow, S. Kurtz, and L. Li. An oracle builder’s toolkit. In *Proceedings of the 8th IEEE Structure in Complexity Theory Conference*, pages 120–131. IEEE, New York, 1993.
- [For94] L. Fortnow. The role of relativization in complexity theory. *Bulletin of the European Association for Theoretical Computer Science*, 52:229–244, February 1994.
- [For97] L. Fortnow. Counting complexity. In L. Hemaspaandra and A. Selman, editors, *Complexity Theory Retrospective II*, pages 81–107. Springer, 1997.
- [FSS84] M. Furst, J. Saxe, and M. Sipser. Parity, circuits and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17:13–27, 1984.
- [Hås89] J. Håstad. Almost optimal lower bounds for small depth circuits. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 143–170. JAI Press, Greenwich, 1989.
- [HHT97] Y. Han, L. Hemaspaandra, and T. Thierauf. Threshold computation and cryptography security. *SIAM Journal on Computing*, 26(1):59–78, January 1997.
- [IR89] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the 21st ACM Symposium on the Theory of Computing*, pages 44–61. ACM, New York, 1989.
- [KM96] S. Kautz and P. Miltersen. Relative to a random oracle, NP is not small. *Journal of Computer and System Sciences*, 53(2):235–250, October 1996.
- [KMR95] S. Kurtz, S. Mahaney, and J. Royer. The isomorphism conjecture fails relative to a random oracle. *Journal of the ACM*, 42(2):401–420, March 1995.
- [LFKN92] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.
- [Lut97] J. Lutz. The quantitative structure of exponential time. In L. Hemaspaandra and A. Selman, editors, *Complexity Theory Retrospective II*, pages 225–260. Springer, 1997.
- [NW94] N. Nisan and A. Wigderson. Hardness vs. randomness. *Journal of Computer and System Sciences*, 49:149–167, 1994.
- [SL96] M. Sheu and T. Long. UP and low and high hierarchies: A relativized separation. *Mathematical Systems Theory*, 29(5):423–449, 1996.
- [TO92] S. Toda and M. Ogiwara. Counting classes are at least as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 21(2):316–328, 1992.

- [Ver93] N. Vereshchagin. Relationships between NP-sets, Co-NP-sets and P-sets relative to random oracles. In *Proceedings of the 8th IEEE Structure in Complexity Theory Conference*, pages 132–138. IEEE, New York, 1993.
- [WT93] O. Watanabe and S. Toda. Structural analysis on the complexity of inverse functions. *Mathematical Systems Theory*, 26:203–214, 1993.
- [Yao85] A. Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science*, pages 1–10. IEEE, New York, 1985.